**Załącznik nr 1.1 do SWZ**

Pakiet 4 - Licencja oprogramowania do systemu cyberbezpieczeństwa

Nazwa producenta: ……………

Typ, model, oraz numer katalogowy: ………………

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Przedmiot zamówienia** | **J.m.** | **Cena jednostkowa netto** | **Stawka podatku VAT** | **Cena jednostkowa brutto** | **Wartość netto** | **Wartość brutto** |
| ***1*** | ***2*** | ***3*** | ***4*** | ***5*** | ***6*** | ***7*** | ***8*** |
| **1.** | ***Zaawansowany system cyberbezpieczeństwa dostarczanego w modelu SaaS, zapewniającego kompleksową ochronę infrastruktury IT organizacji wraz ze wdrożeniem i szkoleniem z administrowania systemem dla personelu Zamawiającego*** | **Przedmiot zamówienia** |  |  |  |  |  |

**Opis przedmiotu zamówienia**

Przedmiotem zamówienia jest dostawa zaawansowanego systemu cyberbezpieczeństwa dostarczanego w modelu SaaS, zapewniającego kompleksową ochronę infrastruktury IT organizacji wraz ze wdrożeniem i szkoleniem z administrowania systemem. System powinien oferować centralną konsolę zarządzania, wysoką dostępność (co najmniej 99,9%) oraz wsparcie dla szerokiej gamy urządzeń, w tym serwerów, stacji roboczych i urządzeń mobilnych. Wszystkie moduły i funkcje muszą pochodzić od jednego producenta, a dane przetwarzane w systemie muszą być zgodne z regulacjami GDPR oraz standardami bezpieczeństwa, takimi jak ISO/IEC 27001:2022 i SOC 2 Type 2. Wymagane jest także, aby system był sklasyfikowany jako rozwiązanie czołowe w uznanych raportach branżowych, takich jak Gartner Magic Quadrant for Endpoint Protection Platforms oraz Forrester Wave for Extended Detection and Response Platforms.

Oczekiwany system powinien integrować moduły odpowiedzialne za detekcję i odpowiedź na zagrożenia (EDR/XDR), ochronę tożsamości użytkowników (ITDR), analizy forensics, zarządzanie incydentami oraz identyfikację podatności w infrastrukturze IT (ASM). System musi zapewniać retencję danych telemetrycznych i logów przez minimum 365 dni oraz oferować szerokie możliwości automatyzacji, takie jak grupowanie alertów, tworzenie scenariuszy obsługi incydentów oraz integrację z narzędziami zewnętrznymi poprzez interfejs API.

System powinien być dostarczony z usługami wsparcia technicznego. Ważnym elementem zamówienia jest potwierdzenie skuteczności rozwiązania w praktyce poprzez jego ocenę w niezależnych raportach branżowych. Dodatkowe punkty oceny ofert mogą być przyznane za rozbudowę funkcji systemu, takich jak większa liczba analiz w sandboxie czy rozwinięcie modułów ochrony tożsamości oraz analizy zagrożeń. Zamawiający przewiduje możliwość dalszego rozwoju funkcjonalności systemu, dostosowanego do indywidualnych potrzeb użytkownika.

**Wymagania ogólne**

1. System musi posiadać centralną konsolę realizowaną w formie usługi SaaS (ang. Software-as-a-Service) o dostępności co najmniej 99,9% a do ochrony stacji i serwerów wykorzystywać agenta.

2. Wszystkie moduły funkcjonalne systemu muszą być dostarczony od jednego producenta.

3. System musi przechowywać i przetwarzać dane na terenie Europejskiego Obszaru Gospodarczego.

4. System musi być zgodny z regulacjami GDPR (ang. General Data Protection Regulation), posiadać certyfikację ISO/IEC 27001:2022 oraz lub zgodność z SOC 2 Type 2.

5. Dojrzałość i skuteczność system musi być poświadczona przez co najmniej następujące niezależne instytucje badające rynek rozwiązań EDR/XDR:

a. System musi być sklasyfikowany przynajmniej jako “Leader” dla raportu Forrester Wave For Extended Detection and Response Platforms Q2 2024.

b. System musi być sklasyfikowany przynajmniej jako „Leader” dla raportu Gartner Magic Quadrant for Endpoint Protection Platforms co najmniej za rok 2023 i 2024.

6. System należy dostarczyć z subskrypcją na okres 36 miesięcy umożliwiającą objęcie ochroną 50 serwerów i 350 stacji roboczych. Jeśli oferowane rozwiązanie licencjonowane jest od liczby użytkowników, to należy przyjąć, że system należy dostarczyć z licencją dla 350 użytkowników z równoczesnym zapewnieniem licencji dla serwerów (50).

7. System musi przechowywać informacje o alarmach i incydentach co najmniej przez 90 dni.

8. System musi przechowywać szczegółowe dane telemetryczne z chronionych systemów w taki sposób, aby możliwe było ich manualne przeszukiwania w konsoli systemu oraz przez interfejs API. Nie dopuszcza się, aby system posiadał jakiekolwiek ograniczenia licencyjne na manualne przeszukiwania w/w danych z konsoli.

9. Interfejs API systemu musi umożliwiać co najmniej następujące akcje:

a. Wykonanie kwerendy do danych telemetrycznych z endpointa i z systemów trzecich

b. Pobranie pliku instalacyjnego agenta

c. Uruchomienie skryptu na wskazanym hoście

d. Zarządzenia izolacją sieciową danego hosta

e. Przywrócenie pliku z kwarantanny

f. Pobranie informacji o alarmach

g. Zlecenie skanowania hosta

h. Pobranie pliku z hosta

10. System musi przechowywać przez 365 dni logi audytowe odnotowujące co najmniej logowanie użytkowników, zmiany wprowadzane w konfiguracji systemu, nawiązywanie zdalnych połączeń do chronionych stacji i wykorzystanie interfejsu API.

11. System musi posiadać możliwość instalacji agenta na co najmniej następujących systemach operacyjnych:

a. Microsoft:

i. Windows 11 (x86-64 oraz arm64)

ii. Windows 10 (x86-64 oraz arm64)

iii. Windows 7 SP1

iv. Windows Server 2003 R2 SP2

v. Windows Server 2008 R2 SP1

vi. Windows Server 2012 i 2012 R2

vii. Windows Server 2016 i Server Core 2016

viii. Windows Server 2019 i Server Core 2019

ix. Windows Server 2022 i Server Core 2022

x. Windows Server 2025 i Server Core 2025

b. Linux

i. Debian 10, 11 i 12

ii. Oracle Linux 8 i 9

iii. Red Hat Enterprise Linux 8, 9 i 10

iv. Rocky Linux 8, 9 i 10

v. SUSE 12 i 15

vi. Ubuntu 18, 20, 22 i 24

c. Apple macOS

i. macOS Ventura 13

ii. macOS Sonoma 14

iii. macOS Sequoia 15

iv. macOS Tahoe 26

d. Apple iOS/iPadOS od 16.x do 18.x

e. Android od 9.x do 15.x

12. System musi posiadać możliwość instalacji agenta na systemach Windows 7 SP1 nie objętych rozszerzonym wsparciem producenta. Wersja agenta dla w/w systemu operacyjnego nie może być wycofana ze wsparcia Producenta otrzymywać bieżące aktualizacje mechanizmów detekcyjno-prewencyjnych.

13. System musi posiadać możliwość instalacji agenta na systemach VDI.

14. System musi umożliwiać wygenerowanie i pobranie pakietu instalacyjnego:

a. W formacie msi lub exe dla systemów Microsoft

b. W formacie pakietu rpm i deb dla systemów Linux

c. W formacie pakietu pkg dla macOS

15. System musi umożliwiać instalację agenta dla systemów iOS/iPadOS i Android za pośrednictwem systemu MDM lub odpowiednio ze sklepu Apple Store i Google Play.

16. Komunikacja między agentem a konsolą systemu musi być realizowana z wykorzystaniem protokołu HTTPS w wariancie co najmniej z TLS1.2 i odbywać się:

a. Bezpośrednio

b. Pośrednio przez proxy systemowe

c. Pośrednio przez proxy wskazane w trakcie instalacji

17. Dokumentacja systemu musi wskazywać adresy IP oraz adresy URL, z którymi komunikuje się agent nawiązując komunikację z konsolą systemu, aby umożliwić udrożnienie komunikacji sieciowej.

18. System musi posiadać możliwość zarządzania przez przeglądarkę internetową. Komunikacja musi być zabezpieczona HTTPS w wariancie co najmniej z TLS1.2.

19. Interfejs webowy systemu nie może korzystać z komponentów typu Flash, Silverlight, applet Java, ActiveX, wtyczek NPAPI.

20. System musi posiadać możliwość zarządzania przez interfejs API. Uwierzytelnienie do interfejsu API platformy musi być realizowane w oparciu o OAuth2 i musi oferować możliwość granularnej autoryzacji dostępu klienta OAuth2 do poszczególnych obszarów funkcjonalnych Systemu.

21. System musi posiadać możliwość wskazania listy publicznych adresów IP, z których będzie istniała możliwość zalogowania się do konsoli systemu oraz nawiązania połączenia do interfejsu API.

22. System musi umożliwiać integrację z zewnętrznymi katalogami użytkowników z wykorzystaniem SAML 2.0.

23. System musi posiadać wbudowany katalog użytkowników oraz obsługiwać drugi czynnik uwierzytelniający wykorzystujący tokeny TOTP (ang. Time Based One-Time Password).

24. System podczas tworzenia haseł dla lokalnych kont administracyjnych musi wymuszać minimalnie następujące wymagania złożoności hasła: co najmniej 11 znaków, musi zawierać małe i duże litery, cyfry i znaki specjalne.

25.System nie może posiadać ograniczenia licencyjnego na liczbę użytkowników (administratorów, analityków, inżynierów bezpieczeństwa) zdefiniowanych w systemie ani ograniczenia na równocześnie zalogowanych w systemie użytkowników. Wszyscy użytkownicy muszą posiadać własne konta imienne. Nie dopuszcza się wykorzystania współdzielonych kont użytkowników.

26. System musi umożliwiać określenie zakresu dostępu z wykorzystaniem matrycy ról i ich przypisania do użytkownika lub do grupy użytkowników. Rola musi definiować dostęp do określonego obszaru administracyjnego systemu, jego rodzaj (tylko do odczytu, pełen dostęp) oraz jego zakresu (wszystkie lub wybrane hosty).

27. System musi obsługiwać co najmniej 5 poziomów ważności alarmów, np: informacyjny, niski, średni, wysoki i krytyczny.

28. System musi automatycznie grupować powiązane alerty w celu przyspieszenia i ułatwienia triażu i analizy incydentu.

29. System musi umożliwiać tworzenie wyjątków dla reguł prewencyjnych na podstawie certyfikatu producenta oprogramowania.

30. System dla alarmów zgrupowanych w ramach incydentu musi automatycznie tworzyć łańcuchy przyczynowo skutkowe reprezentujące zależności pomiędzy procesami wykorzystywanymi w trakcie ataku i powiązane dane telemetryczne, celem ułatwienia przeanalizowania wykorzystywanych technik, określenia zakres ataku, ustalenia celu i zakresu ataku oraz zweryfikowania, czy atak się powiódł.

31. System musi umożliwiać zarządzanie incydentami co najmniej w następującym zakresie:

a. Przypisanie incydentu do analityka

b. Zmianę stanu incydentu np: badany, false positive, true positive, duplikat, testy

c. Dodawanie notatek

32. System musi mapować alarmy do frameworku MITRE ATT&CK.

33. System musi posiadać konfigurowalną możliwość automatycznego uploadowania plików do analizy w sandboxie oraz umożliwiać upload do sandboxa arbitralnych próbek co najmniej przez interfejs API. Wymaga się dostarczyć licencję umożliwiającą upload co najmniej 250 próbek miesięcznie.

34. System musi umożliwiać wgląd w raport z sandboxa dla plików powiązanych z incydentem i eksport raportu.

35. System musi posiadać możliwość kontroli urządzeń podłączanych do portów USB co najmniej na systemach windows i macOS w następującym zakresie:

a. Określenia jakie urządzenia USB można podłączyć

b. Określenia zakresu dostępu do pamięci masowej USB:

i. Brak dostępu

ii. Tylko odczyt

iii. Odczyt i zapis

iv. Odczyt, zapis i uruchamianie

36. System musi posiadać możliwość kontroli host firewalla co najmniej na systemach Windows, MacOS oraz Linux.

37. System musi posiadać możliwość skonfigurowania manualnej i automatycznej aktualizacji agenta dla wskazanych grup hostów. Polityka automatycznej konfiguracji agenta musi umożliwiać określenie:

a. Dnia tygodnia i zakresu czasu, w którym aktualizacja nie będzie wykonywana

b. Tempa propagacji aktualizacji

c. Możliwość wersji: względnie wobec najnowszych wydanych lub bezwzględnie (konkretna wersja)

38. System musi posiadać możliwość kontroli w jaki sposób agent będzie pobierał aktualizacje mechanizmów detekcyjno-prewencyjnych co najmniej w następującym zakresie:

a. Agent pobiera aktualizację natychmiast po opublikowaniu przez producenta

b. Agent pobiera aktualizację z określonym opóźnieniem od momentu publikacji przez producenta

39. System musi umożliwiać dynamiczne grupowanie hostów z wykorzystaniem co najmniej następujących atrybutów: nazwa hosta, domena i OU w Active Directory, system operacyjny, adres IP, podsieć IP, znacznik.

40. System musi umożliwiać nawiązanie zdalnego połączenia konsolowego do hosta chronionego agentem oferując co najmniej następujące funkcje:

a. Podgląd uruchomionych procesów

b. Podgląd systemów plików

c. Podgląd stanu socketów sieciowych

d. Wyłączenie wskazanego procesu

e. Uruchomienie skryptu z biblioteki

f. Pobranie pliku z hosta

g. Wgranie pliku na hosta

h. Zrzut pamięci procesu

i. Zrzut pamięci systemu operacyjnego

j. Wyłączenie i restart systemu

41. System musi umożliwiać zdalną izolację sieciową hosta. W trakcie trwania izolacji sieciowej cały ruch sieciowy z wyjątkiem połączenia do systemu oraz protokołu DHCP musi zostać zablokowany.

42. System musi umożliwiać tworzenie biblioteki skryptów oraz ich zdalne uruchamianie na pojedynczym hoście i na grupie hostów. Wymagana jest obsługa co najmniej następujących języków skryptowych:

a. Systemy windows: powershell

b. Systemy Linux: skrypty bash lub python

c. Systemy MacOS: skrypty zsh lub python

43. System musi posiadać możliwość uruchomienia pełnego skanowania hosta na żądanie i w odpowiedzi na zarejestrowany alarm.

44. System musi umożliwiać bezpośrednią integrację z usługą VirusTotal, DomainTools oraz Security Scorecard. Wraz z Systemem nie jest wymagane dostarczenie licencji do żadnego z w/w narzędzi.

45. System musi umożliwiać globalne oraz per grupa hostów blokowanie uruchamiania plików binarnych poprzez wskazanie ich hasha.

46. System musi posiadać możliwość budowania własnych reguł detekcyjno-prewencyjnych bazujących co najmniej na określeniu łańcucha przyczynowo-skutkowego procesów wraz z określeniem parametrów linii poleceń.

47. System musi posiadać możliwość budowania własnych list indykatorów (ang. Indicator Of Compromise) w formie nazw domenowych, adresów IPv4 i IPv6 oraz hashy SHA256 i MD5 poprzez:

a. Import indykatorów z pliku

b. Manualne dodanie indykatorów

c. Programowe dodanie indykatorów przez interfejs API

48. System musi umożliwiać definiowanie własnych dashboardów (konsol) z wykorzystaniem predefiniowanych widgetów (kontrolek) oraz kontrolek definiowanych samodzielnie poprzez kwerendy do danych telemetrycznych.

49. System musi umożliwiać przeszukiwanie wszystkich danych telemetrycznych przy pomocy kreatorów lub manualnie z wykorzystaniem kwerend. Kwerendy muszą umożliwiać łączenie danych telemetrycznych z różnych źródeł, ich filtrowanie, przekształcanie wyników i obsługiwać free text search (wyszukiwanie dowolnego ciągu znaków bez wskazywania konkretnego pola). Reguły tworzenia kwerend muszą być opisane w dokumentacji systemu.

50. System musi umożliwiać zapisanie kwerendy do danych telemetrycznych do biblioteki.

51. System musi umożliwiać zrealizowanie kwerendy do danych telemetrycznych i odczytanie jej wyników via interfejs API.

52. System musi umożliwiać eksport wyników kwerendy do danych telemetrycznych w formie pliku tekstowego.

53. System musi umożliwiać przekształcenie kwerendy do danych telemetrycznych w uruchamianą zgodnie z podanym harmonogramem regułę korelacyjną generującą alarmy, jeśli kwerenda zwróciła więcej niż jeden rekord.

54. System musi umożliwiać wykrywanie zasobów podłączonych w sieci wewnętrznej w sposób pasywny (analiza tablicy ARP) oraz umożliwiać skonfigurowanie aktywnego skanowania sieci.

55. System musi posiadać następujące możliwości przetwarzania logów z systemów trzecich:

a. Co najmniej 10GB logów dziennie

b. Wsparcie co najmniej dla następujących systemów

i. Windows Event Logs

ii. firewalli Fortinet

iii. VMware ESXi

56. System musi umożliwiać eksport danych telemetrycznych z agenta i danych telemetrycznych z systemów trzecich.

57. System musi posiadać wbudowany moduł SOAR (ang. Security Orchestration, Automation and Response) umożliwiający automatyczną obsługę alarmów w tym m.in. możliwość zmiany konfiguracji (orkiestracji) innych systemów bezpieczeństwa i rozszerzenie kontekstu alarmu poprzez integrację z systemami trzecimi. Wbudowany moduł SOAR musi umożliwiać budowanie spersonalizowanych scenariuszy obsługi (ang. playbooki) z wykorzystaniem graficznego narzędzia bez potrzeby pisania kodu.

58. Wbudowany moduł SOAR musi posiadać możliwość orkiestracji systemów bezpieczeństwa wewnątrz sieci Zamawiającego (systemów on-prem) oraz systemów bezpieczeństwa dostarczanych w formie usługi chmurowej (systemy SaaS).

59. Wszystkie moduły funkcjonalne systemu muszą być dostarczone z takim samym okresem licencji tj. na okres 36 miesięcy.

**Wymagania dla agenta**

60. Agent nie może wykorzystywać Oracle Java JRE/JDK.

61. Instalacja agenta nie może wymagać restartu systemu operacyjnego.

62. Agent musi weryfikować poprawność certyfikatu w trakcie nawiązywania połączenia z systemem w celu ochrony przed atakami man-in-the-middle z wykorzystaniem mechanizmu certificate pinning lub podobnego.

63. Agent musi posiadać mechanizmy ochronne uniemożliwiające wyłączenie agenta lub wpłynięcie na jego poprawne funkcjonowanie nawet przez użytkowników z podwyższonymi uprawnieniami (ang. anti-tampering) na systemach Windows, macOS i Linux.

64. Odinstalowanie agenta musi być chronione unikalnym hasłem dla każdej chronionej stacji, tak aby uniemożliwić odinstalowanie agenta nawet użytkowników z podwyższonymi uprawnieniami na systemach Windows, macOS i Linux.

65. W trakcie instalacji agenta musi istnieć możliwość nadania agentowi nieusuwalnego bezpośrednio z konsoli systemu znacznika, który może zostać wykorzystany jako atrybut do grupowanie hostów.

66. W trakcie instalacji agenta musi istnieć możliwość wskazania dedykowanego serwera proxy, z którego agent będzie korzystał nawiązując połączenie z systemem.

67. Agent musi wykrywać i blokować próby wyłączenia usługi Volume Shadow Copy Service (VSS) oraz inne próby uszkodzenia migawek VSS.

68. Agent musi realizować ochronę przed atakami klasy Bring Your Own Vulnerable Driver poprzez wykrywanie i blokowanie prób ładowania podatnych sterowników.

69. Agent musi bezpośrednio na chronionym hoście zapewniać ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi co najmniej w następujący sposób:

a. Weryfikacja reputacji pliku w bazie threat intelligence producenta systemu

b. Lokalna analiza statyczna bazująca na uczeniu maszynowym (ang. Machine learning)

70. Agent musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi makrami w plikach Microsoft Word i Microsoft Excel co najmniej w następujący sposób:

a. Weryfikacja reputacji makra w bazie threat intelligence producenta

b. Lokalna analiza statyczna bazująca na uczeniu maszynowymi (ang. Machine learning)

71. Agent musi posiadać możliwość usuwania złośliwych makr wykrytych w plikach Microsoft Word i Microsoft Excel.

72. Agent musi realizować ochronę przed zaszyfrowaniem dysku i plików przez złośliwe oprogramowanie (aka ochrona anty-ransomware’owa).

73. Agent musi wykonywać analizę plików binarnych po tym jak zostały zapisane w systemie plików.

74. Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu.

75. Agent musi posiadać konfigurowalną opcję umieszczania złośliwych plików w kwarantannie.

76. Agent musi automatycznie wykonywać skanowanie pamięci masowej natychmiast po jej podłączeniu do portu USB lub musi blokować próby intencjonalnego i automatycznego uruchomienia plików wykonywalnych z pamięci masowej.

77. Agent musi posiadać mechanizm skanowania pamięci RAM w celu wykrywania złośliwego kodu.

78. Agent, poprzez analizę złożonych łańcuchów przyczynowo skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców, musi zapewnić ochronę przed atakami klasy Living of The Land wykorzystującymi legalne narzędzia systemowe w groźny sposób.

79. Agent musi zapewniać ochronę przed atakami mającymi na celu kradzież poświadczeń użytkowników.

80. Agent musi posiadać możliwość automatycznej remediacji złożonych ataków co najmniej poprzez wyłączenie złośliwych procesów, umieszczenie plików w kwarantannie, usunięcie zadań z harmonogramu i wpisów z rejestru.

81. Agent musi integrować się z Windows Security Center.

82. Agent musi umożliwiać kwarantannę groźnych plików.

83. Agent musi działać:

a. W jądrze systemu (używać sterownika) na systemach Windows

b. W jądrze systemu (aka kernel space) lub poza jądrem systemu (aka user space) na systemach Linux

c. Poza jądrem systemu na systemach MacOS

84. Agent dla systemów Windows, MacOS i Linux musi zbierać i wysyłać do systemu co najmniej następujące dane telemetryczne:

a. Utworzenie nowego procesu i zakończenie procesu

b. Operacje na socketach sieciowych dla TCP i UDP

c. Operacje na plikach

d. Zdarzenia z event logu dotyczące uwierzytelnienia.

e. Operacje na rejestrze (tylko systemy Windows)

85. W przypadku braku łączności z systemem agent musi lokalnie przechować dane telemetryczne i wysłać je do systemu po przywróceniu łączności sieciowej.